UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

MOOG INC., Plaintiff, v. SKYRYSE, INC., ROBERT ALIN PILKINGTON, MISOOK KIM, and DOES NOS. 1-50, Defendants.	Case No. 22-187

MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFF'S MOTION FOR A TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

PRELIMINARY STATEMENT

Unmanned helicopter aviation, which both Plaintiff Moog Inc. ("Moog") and Defendant Skyryse, Inc. ("Skyryse") are pursuing, is a new market, but one for which the underlying technology requires years of development and investment of millions of dollars. Moog has for decades developed software that governs flight controls for airplanes and other aircrafts, including helicopters. Skyryse is a start-up founded in 2016, which in 2019 pivoted its business model to develop the exact technology that it had proposed engaging Moog to perform subject to non-disclosure agreements between the parties in 2018 and 2019. In Fall 2020, Skyryse received over $200 million of new investment, and with it, heightened expectations from investors to deliver, and quickly. Faced with the realization that it could not "win" on its own, Skyryse has elected to unfairly compete by taking what it could not develop fast enough. This case arises out of a strategic plundering by Skyryse of Moog's proprietary and trade secret information and raiding of Moog's software engineer team to give Skyryse, in as short a time as possible, an unfair competitive edge in launching its own unmanned helicopter aviation offerings.

As part of its strategy, Skyryse has to date hired away over twenty Moog employees (of a team of approximately fifty), including Defendant Robert Alin Pilkington ("Pilkington"), lead architect on the second iteration of Moog's Platform base software for military purposes, and Defendant Misook Kim ("Kim") (collectively with Skyryse and Pilkington, "Defendants") who worked for Pilkington. On behalf of Skyryse, Pilkington instructed Defendant Kim, a senior staff engineer at Moog, to copy on November 19, 2021 over 136,000 files of Moog's proprietary, confidential, and trade secret data to an external hard drive, including all source code for Moog's Platform base software and related project-specific applications, representing years of invaluable development and investment of millions upon millions of dollars, just weeks before she left Moog to join Skyryse. In short, Skyryse has taken virtually everything that

Moog's flight control software engineering group developed over the past 15 years.

Since the theft, Defendants have engaged in a blatant cover up. After multiple requests by Moog, Kim returned two separate external hard drives, both of which were completely wiped clean. An expert forensic inspection of the two hard drives and Kim's two Moog-issued laptop devices reveals: 1) the hard drive used to copy over 136,000 files of Moog's data had been intentionally formatted sometime after Kim's departure from Moog such that it is impossible to determine the contents of the drive or if any data was copied or transferred elsewhere; 2) Kim copied additional Moog data on December 15, 2021, and 54 GB of data was deleted from one of Kim's computers just two days later (her last day at Moog); 3) there is a third external hard drive used by Kim during the relevant period which has not been returned to Moog; and 4) the initial false hard drive returned to Moog had been re-named to resemble the actual hard drive that was used in copying Moog's data. Further, the back covers of Kim's two Moog-issued laptop devices indicate they have been removed (which allows removal of its hard drives). Defendants stole Moog's data multiple times, used and manipulated multiple devices to escape detection, and erased their tracks so Moog cannot determine what happened to its stolen data.

The evidence shows Moog will likely succeed on the merits of its affirmative claims. If Defendants are not stopped immediately, Moog faces irreparable harm in the form of lost market share, damaged client relationships and goodwill, and the irreversible disclosure of its trade secrets. Both temporary and preliminary injunctive relief should be awarded.

STATEMENT OF FACTS

Founded in 1951 in East Aurora, New York, Moog is a publicly traded (NYSE: MOG.A, MOG.B) aerospace and defense company. Moog designs and manufactures electric, electro-hydraulic and hydraulic motion, controls and systems for three segments: aircraft controls, space

and defense controls, and industrial controls. Moog has developed the flight control systems used on some of the most common commercial aircrafts, including the Boeing 747 and Airbus A350. Moog has over 10,000 employees and sales, engineering, and manufacturing facilities in 26 countries. Skyryse, founded in 2016 in Los Angeles, is an aerospace start-up company.

A Moog's Flight Control Software

Moog designs and manufactures the most advanced motion control products for aerospace, defense, industrial and medical applications. (Hunter Dec., ¶ 5). Moog develops flight control software for aircrafts, including helicopters. (*Id.*, ¶ 6). Essentially, Moog develops software that pairs up with the hardware computer contained in an aircraft to control its flight and navigation functionality. For example, when a pilot moves a control well in the cockpit, Moog's software reads the control and moves the particular component of the airplane. (*Id.*, ¶ 7).

Moog's base flight control software is called Platform. (Hunter Dec. ¶ 8; Schmidt Dec., ¶ 5). Platform is the "operating system" that an aircraft's computer uses, similar to Windows or Mac OS for a standard home computer. (*Id.*). Moog then builds applications specific to the particular aircraft to sit on top of the Platform base operating system to tailor its functionality to the particular aircraft. (*Id.*). The particular application provides a specific use, but the underlying operating system allows the entire system and machine to work. (*Id.*). Over the past 15 years, Moog has developed three major branches of the Platform base flight control operating system software: (i) commercial aircrafts, (ii) military use (called "eRTOS"), and (iii) motor applications (called "AMP"). (Hunter Dec. ¶ 9) (Schmidt Dec. ¶ 6). Building each iteration of the Platform software required 10 full-time software engineers over a period of two to three years. (*Id.*).

B Platform's Immense Value to Moog

The Platform base software, and related project-specific applications, constitute Moog's most valuable, sensitive, and proprietary information. (Hunter Dec. ¶ 12). The types of

information relating to Platform and related project-specific applications that Moog always treats as internal trade secrets which are never disclosed to other parties are: 1) the source code for these programs; and 2) certain documents and checklists prepared by Moog's Software Engineering Process Group ("SEPG"), which contain processes to ensure that the software is being developed in a manner to meet certification requirements by the Federal Aviation Administration ("FAA") and other similar authorities around the world. (*Id*., ¶ 28). The SEPG documents have been optimized over 20 years of working with aviation authorities around the world. (*Id*.). Many companies hire Moog for software development specifically because Moog knows how to efficiently certify software to meet governing aviation standards. (*Id*.).

Platform allows Moog to be a front-runner in obtaining bids from commercial or military parties (*Id*., ¶ 13). Other competitors do not have this level of adaptable base software which allows project-specific applications to be developed so quickly on top of an existing base software. (*Id*.). On top of the multiple years it took to build Platform, the testing requirements for flight control software are extremely vigorous and costly. (*Id*., ¶ 15). Before any flight control software is approved by the FAA or similar governing bodies, it must be vigorously tested and certified. (*Id*.). It takes double the resources to certify a flight software than it does to construct it, and this process constitutes two-thirds of Moog's total cost to build flight software. (*Id*.).

If a third party obtained Moog's Platform software and underlying code, testing, and certification requirements, it could "click and build" project-specific software on top of the base software in a short amount of time. (*Id*., ¶ 18).

C Efforts to Keep Moog's Flight Control Software Secret

Many Moog employees are required to sign Moog internal proprietary information agreements, as well as third party proprietary information agreements when working on certain project-specific applications. (*Id*., ¶ 20). Every employee is required to periodically review and

sign an acknowledgement in writing of the then-current Moog employee handbook (the "Employee Handbook"). (*Id*., ¶ 21). Pilkington acknowledged its receipt and agreed to abide by its policies on July 30, 2012, and Kim acknowledged its receipt on January 21, 2013. (*Id*., Ex. A). The employee handbook provides, among other things, that: 1) Moog employees will receive access to confidential and proprietary information; 2) disclosure to any outside party is prohibited, including after employment has been terminated; and 3) Moog employees may not retain any copies of Moog's confidential and proprietary information. (*Id*., Ex. B at pp. 58-59).

Moog also has robust written policies regarding its confidential, proprietary, and trade secret information made available to every Moog employee, and Moog requires its software engineers to regularly complete trainings regarding company "trade secrets" which summarizes the contents of its written IP policies. (*Id*., ¶ 24, Exs. C, D). Pilkington and Kim attended these trainings multiple times. (*Id*., Ex. E). Moog also requires its departing employees to sign an exit form where each individual confirms they have been provided access to Moog's proprietary and trade secret information, have returned all Moog IP upon departure, and have not maintained access to any digital record of Moog. (Daly Dec., Ex. A at p. 3).

Platform is housed on a secure server at Moog's East Aurora, New York offices. Not all employees at Moog have access to the software database. (Hunter Dec. ¶ 25). Access to the software database is on a "need to know" basis that must be approved by the lead on software program. (*Id*., ¶ 26). In order to have access to Platform and related project-specific software, a Moog employee would need five separate credentials. (*Id*., ¶ 27). Further, certain US Government programs require heightened security credentials which take a long time to obtain.[1]

[1] Moog has obligations under its government contracts to implement extensive security measures to safeguard and protect sensitive information, including but not limited to, access restrictions, authentication, encryption, physical protections, and specific training for employees. Moog also employs additional requirements and protections for sensitive data for certain of its government customers.

(*Id*., ¶ 65). Moog also has several physical security measures to safeguard its proprietary information, including controlled access into buildings, mandatory security screenings for all employees, and background checks before hiring. (*Id*., ¶ 22). Finally, Moog source code files are designated "MOOG PROPRIETARY and CONFIDENTIAL INFORMATION" and contains restrictive language prohibiting its disclosure to third parties. (*Id*., ¶ 29).

D Relevant Moog Team That Developed Platform

Gonzalo Rey (former Director of Engineering and Chief Technology Officer) and Sathya Achar (former Engineering Technical Fellow) were the first two Moog employees to sponsor and oversee the development of Moog Platform base software beginning in 2007. (Hunter Dec. ¶ 30). They have the most institutional and technical knowledge regarding the software, as well as its relationship with project-specific applications which sit on top of the base software. (*Id*.).

Michael Hunter and Todd Schmidt are two senior level engineers who have worked on and managed the programs that created Platform and related applications, since 2007. (Hunter Dec. ¶¶ 3-4) (Schmidt Dec. ¶¶ 3-4). Robert Alin Pilkington (former Senior Staff Engineer) was the lead architect on eRTOS. (Hunter Dec. ¶ 31). Pilkington reported to Hunter and Schmidt during his tenure at Moog. (Hunter Dec. ¶ 31) (Schmidt Dec. ¶ 24). Misook Kim was a Senior Staff Engineer who worked under Pilkington. (Hunter Dec. ¶ 31).

E Moog and Skyryse's Initial Business Relationship

In 2018, Moog's Growth & Innovation Group (focused on finding new and innovative business opportunities for Moog outside of its existing business channels) began exploring a potential business opportunity with Skyryse. (Stoelting Dec., ¶ 7). Skyryse indicated it wanted offer on-demand helicopter transportation to the general public, through the use of automated flight system technology. (*Id*., ¶ 9). Under this proposed structure, Moog would provide the automated helicopter flight control systems (including flight control software, actuators, and

computers), and Skyryse would install and implement this technology into their business. (*Id*.). This proposal was appealing to Moog, providing a new business channel that would capitalize on Moog's decades of experience in developing flight control systems. (*Id*.).

Moog and Skyryse entered into two separate Non-Disclosure Agreements on October 24, 2018 (the "2018 NDA") and March 15, 2019 (the "2019 NDA") (collectively, the "NDAs"). (Stoelting Dec. ¶¶ 12-13, Exs. A, B). Under those NDAs, the Parties agreed not to disclose any proprietary information disclosed by the other parties, refrain from any reverse engineering, and the receiving party of such information could only be used for the limited purpose of the contemplated engagement between Moog and Skyryse. (*Id*., § 2).

Moog and Skyryse's business relationship was to be conducted in four separate phases. On May 31, 2019, the Parties entered into a [redacted]

On June 3, 2019, Moog and Skyryse entered into a corresponding [redacted]

F Skyryse's Changes Its Business Model to Overlap with Moog's

Moog met its obligations and timely provided to Skyryse the deliverables under the SOW. (Stoelting Dec. ¶ 21). However, Skyryse's planned launch in October 2019 failed as it stopped its business operations, fired many of its employees, and pivoted its business model. (*Id*., ¶ 22). In late 2019, Skyryse began advertising that it was offering an autonomous flight system

as part of a flight control operating system. (*Id*., ¶ 23). Skyryse called its flight operating system "Luna," which was very similar to Moog's name for its autonomous flight system previously discussed with Skyryse, "Lucy." (*Id*.). It became clear to Moog that Skyryse had now pivoted into developing exactly the technology that it had proposed engaging Moog to perform. (*Id*.).

On May 22, 2020, Skyryse issued a request for quote ("RFQ") to Moog. (Stoelting Dec. ¶ 24, Ex. E). Skyryse requested that Moog provide flight control computers and actuator systems for Skyryse to use and to implement Skyryse's flight control operating system software. (*Id*., ¶ 25). This was already an established line of business for Moog, so Moog's Growth & Innovation Group was reluctant to move forward. (*Id*.). Nonetheless, given the prior business relationship with Skyryse, and the fact that several former Moog employees worked at Skyryse, on September 22, 2020, Moog submitted a bid in response to Skyryse's RFQ for $46,195,870. (*Id*., ¶ 26, Ex. F). Skyryse advised Moog that its bid was too expensive and declined. (*Id*., ¶ 27). Phase 1 concluded, but the terms of the 2018 and 2019 NDAs were never terminated. (*Id*., ¶ 28).

G Skyryse's Raiding of Moog's Employees

To date, Skyryse has hired 20 software engineers from Moog, with the majority of these departures occurring in the past few months. (Hunter Dec. ¶ 34). Rey was the first Moog employee to join Skyryse when he left Moog in 2017. (*Id*.). Achar joined Skyryse in January 2022, after advising Moog that he was retiring. (*Id*.). Pilkington left Moog on November 12, 2021 to join Skyryse. (*Id*.). These key, senior individuals are extremely familiar with Moog's Platform base software and related project-specific applications, as well as the more capable members of Moog's software engineering teams who worked on these programs. (*Id*., ¶ 35).

Kim left Moog on December 17, 2021 to join Skyryse. (*Id*., ¶ 34). Several additional software engineers have followed suit. Skyryse has reached out to a large number of software engineers at Moog, primarily targeted at Moog's Los Angeles-area office. (*Id*., ¶ 38).

While some engineers have remained loyal to Moog, Skyryse has aggressively recruited them as well. For example, in August 2021, Rey contacted Hunter and asked him to join Skyryse. (*Id*., ¶ 36). In January 2022, Pilkington reached out to Hunter asking him to join Skyryse. (*Id*., ¶ 37). Pilkington advised Hunter that there was "urgency" at Skyryse. (*Id*.).

Similarly, on October 13, 2021, Rey contacted Schmidt to see if he would join Skyryse as lead engineer. (Schmidt Dec. ¶ 9). Rey told Schmidt something to the effect of: "You will become very wealthy." (*Id*., ¶ 11). During a phone call, Rey advised Schmidt that Skyryse's goal was extracting flight control functions to an iPad type of interface, so that anyone who can use an iPad can fly a helicopter. (*Id*., ¶ 10). Rey also advised that Skyryse wanted to provide an entire system that could fly an aircraft, including hardware and software components (*Id*.).

H Substantial Data Theft of Moog's Most Proprietary Information

Moog recently discovered that on November 19, 2021, between the hours of 3:00 and 7:00 a.m. and from a remote location, former Moog employee Kim copied certain Moog data to an external hard drive. (Bagnald Dec., ¶¶ 8, 10). This event took place less than one month before Kim's last day at Moog, and less than one week after Pilkington, her supervisor, left Moog for Skyryse. (*Id*.). Kim copied 136,994 separate files:

Type	Number
Source Code	43,960
Spreadsheets	5,377
Documents	2,831
Executables	954
Images	9,003
MAP Files	2,010

Models	7,898
Object Files	1,026
Plain Text	4,613
Presentations	404
Misc.	20,655
SVN Logs	38,263
Total Files	**136,994**

(*Id*., ¶ 13). Kim used Pilkington's file path to copy the data onto the external hard drive. (Bagnald Dec. ¶ 14) (Hunter Dec. ¶ 47) (Schmidt Dec., ¶ 23). Employees working on Platform had their own "branch" or location on Moog's server, to store sensitive materials they needed access to. (*Id*.). The file path used by Kim was: "D:\Misook\ENG_Alin_Branch\Software…" (*Id*.). Kim had credentials to use her own file path, but instead used Pilkington's. (*Id*.).

Several Moog senior engineers confirmed that Kim was very loyal to Pilkington, and would do anything he instructed. (Hunter Dec. ¶ 51; Schmidt Dec. ¶¶ 24-25; Lopez Dec., ¶ 6). Kim would not have accessed Pilkington's branch unless he expressly instructed her to. (*Id*.).

I Nature and Value of the Copied Data

The scope of data copied by Kim is remarkable. Moog senior engineers Messrs. Hunter and Schmidt have analyzed the file log of data copied by Kim (the "File Log"). (Hunter Dec. ¶¶ 42-43) (Schmidt Dec. ¶¶ 18-19). The entire application layer for Platform was copied by Kim, meaning that 100% of the base Platform software and its code were copied. (Hunter Dec. ¶ 45) (Schmidt Dec. ¶ 21). All three iterations (commercial, military, motors) of Platform were copied, as well as test artifacts (*Id*.). Kim copied the entire application layer for seven project-specific applications, including six military projects. (*Id*.). This comprises all of the code,

documentation, and related information regarding the composition, testing, and certification of Platform and project-specific applications. (Hunter Dec. ¶ 46) (Schmidt Dec. ¶ 22) (Lopez Dec. ¶ 11). Additionally, in addition to source code, Kim copied Moog's trade secret checklists (76) and five documents from its SEPG repository. (Hunter Dec. ¶ 46). Kim essentially copied everything that Moog's flight control software engineering teams had worked on over the past 15 years. (Hunter Dec. ¶ 63) (Schmidt Dec. ¶ 27) (Lopez Dec. ¶ 14).

J No Legitimate Purpose for Kim's Data Copying

There was no legitimate purpose for Kim's copying of Moog's proprietary, confidential, and trade secret information. Kim signed an exit form (the "Exit Form") on her last day at Moog, December 17, 2021, where she affirmed in writing that she had returned all Moog "TRADE SECRET/COMPANY CONFIDENTIAL INFO." (Daly Dec., Ex. A). The Exit Form also provides, among other things: 1) Kim "owes a fiduciary duty to Moog to not usurp any such corporate opportunity for [her] own benefit"; and 2) Kim affirms that she does "not maintain access to, or have possession of, any tangible or digital record of Moog IP-whether in hard copy or digital form—on any device, cloud, or digital storage facilities." (*Id.*).

Regardless, the standard way in which Moog employees worked on Platform-related projects would be connecting to Moog's server via remote virtual private network ("VPN"). (Hunter Dec. ¶ 27). All of the data copied by Kim is located on Moog's internal servers in East Aurora, New York. Even if Kim was working on a different Moog computer, she could access all the data she copied from Moog's Subversion network using her login credentials. (Schmidt Dec ¶ 32). Even if downloading data was necessary, a copy of the data would be stored to the user's hard drive on their laptop computer – not an external hard drive. (Hunter Dec. ¶ 48).

Further, in December 2021, Kim was working solely on a military program labeled herein as "Sensitive Government Program 2." (Hunter Dec. ¶ 54) (Schmidt Dec. ¶ 31) (Lopez

Dec., ¶ 15). Kim was a software tester, not an engineer who wrote code. (Hunter Dec. ¶ 49). Thus, even if Kim wanted to copy certain Moog data for legitimate business purposes, she would only have a need to copy certain verification and testing data related to Sensitive Government Program 2 (instead of the entire application layer for several projects she never touched). (Schmidt Dec. ¶ 31). To support legitimate business purposes, Kim would have needed, at most, to access only 0.5% of the total data that she copied on November 19, 2021. (*Id*.).

K Kim Returns Two Hard Drives Which are Both Wiped Clean

When contacted by Moog, Kim engaged in a cover up in an attempt to mask her actions. On January 28, 2022, Moog informally requested that Kim return the company-issued external hard drive she had in her possession. (Bagnald Dec. ¶ 15). On January 31, 2022, Kim's sister who also works at Moog returned on Kim's behalf a hard drive to Moog. (*Id*.). However, a quick inspection of this device revealed it was not the device Kim used to copy Moog's data on November 19, 2021, ***and*** it had been completely wiped clean. (*Id*., ¶¶ 11, 16-17).

On February 18, 2022, Moog sent a formal letter to Kim demanding that she return the external hard drive in question. (Daly Dec. ¶ 5, Ex. B) Kim called Moog's HR employee Jamie Daly, advising her that she had possession of the Moog external hard drive, and that she downloaded a large set of files in order to help Moog employees after her departure. (*Id*. ¶ 7). Kim claimed she needed the files for Sensitive Government Program 2. (*Id*.).[2] She then stated she had deleted all of the files on the drive. (*Id*.). Moog then recovered the hard drive. (*Id*., ¶ 8).

An expert forensic analysis was performed on Kim's two hard drives and two Moog-issued laptops which revealed: 1) the hard drive used to copy over 136,000 files of Moog's

[2] This explanation makes no sense because, among other reasons: 1) there was no plan or agreement for Kim to assist Moog employees after her departure; 2) at the time of departure, Kim was only working on testing related to Sensitive Government Program 2, and therefore was only involved in at most 0.5% of the total data she copied; 3) Kim returned a different hard drive the first time without any mention of the actual hard drive in question; and 4) Kim should have disclosed the data she copied on her Exit Form. (Hunter Dec. ¶¶ 52-57).

data had been intentionally formatted sometime after Kim's departure from Moog in such a manner that it is impossible to determine the contents of the drive or if any data was copied or transferred to another device; 2) Kim copied additional Moog data to the same hard drive on December 15, 2021, and 54 GB of data was deleted from one of Kim's computers just two days later; and 3) there is a third external hard drive used by Kim during the relevant period which has not been returned to Moog; and 4) the initial false hard drive returned by Kim's sister had been re-named in an effort to resemble the second hard drive which was used to actually copy Moog's data. (*See generally* Pixley Dec.). Further, the back covers of Kim's two Moog-issued laptop devices indicate they have been removed (allowing removal of its hard drives). (Johnnie Dec., ¶¶ 11-13, Exs. C, D).

ARGUMENT

I. MOOG REQUIRES TEMPORARY AND PRELIMINARY INJUNCTIVE RELIEF

Pursuant to Rule 65 of the Federal Rules of Civil Procedure and L.R.Civ.P. 65, Moog seeks a temporary restraining order (i) prohibiting Defendants from using, accessing, disclosing, copying, or transmitting Moog's trade secrets and other proprietary information; (ii) requiring the return of all such information in Defendants' possession, custody, or control to Moog, and (iii) requiring the preservation of Defendants' electronic devices, accounts, and networks for evidentiary purposes. Moog also seeks a preliminary injunction prohibiting Defendants from (i) continuing to possess or use Moog's confidential, proprietary, and/or trade secret information; and (ii) such other relief as the Court may deem appropriate as against Defendants. The same standard governs both an application for a temporary restraining order and an application for a preliminary injunction. *Jones v. Wolf*, 467 F. Supp. 3d 74, 81 (W.D.N.Y. 2020). A plaintiff "'must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of

equities tips in his favor, and that an injunction is in the public interest.'" *Id.* (internal citations and quotation marks omitted).

II. MOOG WILL SUFFER IRREPARABLE HARM IF TEMPORARY AND PRELIMINARY INJUNCTIVE RELIEF IS NOT GRANTED

Moog's threated injury is irreparable, as it is "neither remote nor speculative, but actual and imminent and that cannot be remedied by an award of money damages." *See trueEX, LLC v. MarkitSERV Ltd.*, 266 F. Supp. 3d 705, 726 (S.D.N.Y. 2017) (internal citations and quotation marks omitted). Indeed, "[a] trade secret once lost is, of course, lost forever" and, as a result, such a loss "cannot be measured in money damages." *FMC Corp. v. Taiwan Tainan Giant Indus. Co.*, 730 F.2d 61, 63 (2d Cir.1984); *see Computer Assocs. Int'l v. Bryan*, 784 F. Supp. 982, 986 (E.D.N.Y.1992) (same).

The loss of Moog's reputation as a first-mover in the market, Defendants' theft of Moog's source code and trade secrets, and damage to Moog's goodwill and customer relationships are precisely the types of irreparable harm that courts in the Second Circuit have issued injunctive relief to redress. *See, e.g., Lumex, Inc. v. Highsmith*, 919 F. Supp. 624, 636 (E.D.N.Y. 1996) ("The potential loss of an industry leader's present market and loss of the advantage of being the pioneer in the field and the market leader, may constitute irreparable harm."); *see also PLC Trenching Co., LLC v. Newton*, No. 6:11-CV-0515, 2011 WL 13135653, at *3 (N.D.N.Y. Dec. 12, 2011) (finding irreparable harm where use of plaintiff's trade secrets "would harm Plaintiff in a way that cannot easily be measured in dollars."); *Asa v. Pictometry Int'l Corp.*, 757 F. Supp. 2d 238, 244-245 (W.D.N.Y. 2010) (loss of "customer goodwill" and "[m]ajor disruption of a business" can "quality as irreparable injury."). This is not a case where Moog lost one or two sensitive documents—Defendants surreptitiously copied 15 years' worth of proprietary software code and related data, nearly 137,000 files' worth.

A The Unmanned Helicopter Aviation Market and High Barriers to Entry

Unmanned helicopter aviation, which both Moog and Skyryse are pursuing, is a new market with no industry leader. (Hunter Dec. ¶ 59). About 20 companies, including Moog and Skyryse, are pursuing the market. (*Id*.). Whichever company is first to market with a viable product will likely win substantial market share just by wont of being first. By stealing Moog's source code and other proprietary information underlying Platform and related applications, and crippling Moog's software engineering workforce, Skyryse has unlawfully jumped to the front of this race. This harm to Moog is irreparable, because time cannot be unwound.

Further, there is a high barrier to entry in the flight control software market. (*Id*., ¶ 60). Companies that have an established, tested, and proven software and have successfully delivered on contracts have a huge advantage in securing contracts from the government and other third parties. (*Id*.). Other companies would have to pay two to three times what Moog does to secure a flight control software contract because Moog has established flight control operating system software. (*Id*., ¶ 61). Moog wins most of the flight control projects that it bids on. (*Id*.).

If a third party such as Skyryse obtained the entire code and underlying data to Moog's Platform software and related applications, the large barrier to entry would be removed because it would save Skyryse tens of millions of dollars and decades of work in avoided development efforts. (*Id*., ¶ 63). Some of the project-specific applications copied by Kim, including G280, are directly relevant to Skyryse's business. (Hunter Dec. ¶ 61) (Schmidt Dec. ¶ 28).

Kim essentially copied every piece of data related to every flight control software and application developed by Moog over 15 years. (Hunter Dec. ¶ 63; Schmidt Dec. ¶ 27). This data is the epitome of priceless and represents the highest level of intelligence and wisdom of Moog's premier engineers and software architects of the past two decades. (Schmidt Dec. ¶ 27).

B Moog's Enormous Investment in its Flight Control Programs

Moog's investment of engineering time, money, and other resources into the development, testing, and certification of its programs and applications has been enormous. Moog has invested approximately [redacted] in developing, testing, and certifying all three iterations of its Platform base software over the past 15 years. (Hunter Dec. ¶ 16). Moog has also invested approximately [redacted] in developing, testing, and certifying its aircraft project-specific software applications that sit on top of the Platform software. (*Id*.).

For context, Moog's flight control systems for a commercial aircraft (including software, hardware, actuation, hydraulics, etc.) typically cost between [redacted] for each type of aircraft, which in turn require over one million hours of software engineering and support staff time. (Schmidt Dec. ¶ 15). For example, Kim copied all data related to the eRTOS iteration of the Platform base software. (Lopez Dec. ¶ 11). [redacted] (*Id*. ¶ 13). Just writing the code for eRTOS took multiple years. (*Id*.). Once written, it still takes several additional years to verify, test, and certify the code under Federal Aviation Administration and other international governing body standards. (*Id*.). As another example, Kim copied all data related to Sensitive Government Program 1, [redacted] (*Id*., ¶ 12).

C Moog Has Suffered Substantial Reputational Harm and Loss of Goodwill

Defendants' misappropriation, if not promptly enjoined, will jeopardize and irreparably impair Moog's ability to obtain future commercial and government contracts. (Hunter Dec. ¶ 67). Under every contract that Moog enters into for flight software development, Moog must notify its customers if certain proprietary or confidential data is copied or stolen. (*Id*., ¶ 66). Indeed, data and information security is of paramount concern in this industry, especially with the US Government. (*Id*. ¶ 67). Defendants' theft of Moog's data puts its sterling reputation

into jeopardy. (*Id.*). *See Eastview Mall LLC v. Grace Holmes Inc.*, 122 N.Y.S. 3d 848, 851 (2020) ("loss of goodwill and damage to customer relationships, unlike the loss of specific sales, is not easily quantified or remedied by money damages."); *Velo-Bind, Inc. v. Scheck*, 485 F. Supp. 102, 109 (S.D.N.Y. 1979) (noting that good will built up over the years is not monetarily ascertainable, and issuing injunctive relief). Absent immediate judicial relief to stop the use of these materials, this reputational and goodwill harm will continue and increase in severity.

D Defendants Will Inevitably Use and Disclose Moog's Trade Secrets

Moog can also demonstrate irreparable harm because there is a high probability that Defendants will "inevitably disclose" Moog's trade secrets and proprietary information. *Int'l Bus. Machines Corp. v. Papermaster*, No. 08-CV-9078(KMK), 2008 WL 4974508, at *8 (S.D.N.Y. Nov. 21, 2008). Under the inevitable disclosure doctrine, irreparable harm may be found even when there is no proof that a defendant has actually misappropriated trade secrets if there is a substantial risk that he will do so in his new employment setting. Courts consider the following factors: "(1) the extent to which the new employer is a direct competitor of the former employer; (2) whether the employee's new position is nearly identical to his old one, such that he could not reasonably be expected to fulfill his new job responsibilities without utilizing the trade secrets of his former employer; (3) the extent to which the trade secrets at issue would be valuable to the new employer; and (4) the nature of the industry and its trade secrets." *Int'l Bus. Machines Corp. v. Lima*, No. 7:20-cv-4573, 2020 WL 5261336, at *12 (S.D.N.Y. Sep. 3, 2020) (citing *Papermaster*, 2008 WL 4974508, at *7).

Here, each factor supports application of the inevitable disclosure doctrine against Pilkington and Kim. First, Moog and Skyryse are direct competitors in the unmanned flight control software market. *Cf. Lima*, 2020 WL 5261336, at *12 (granting injunctive relief based on the inevitable disclosure doctrine because IBM and Microsoft "engage in head-to-head

competition"). Second, Pilkington and Kim's new positions at Skyryse are comparable to their former positions at Moog. At Moog, Pilkington was the lead architect on the second iteration of Moog's Platform base software for military purposes, and Kim was a senior staff engineer. Their roles at Skyryse involve the same type of work, such that they cannot reasonably be expected to fulfill their new job responsibilities without utilizing Moog's confidential information. *See Lima*, 2020 WL 5261336, at *12 (granting injunctive relief based on the inevitable disclosure doctrine because defendant Mr. Lima's "proposed employment at Microsoft is nearly identical to that at IBM," as "Mr. Lima's proposed job will be to execute global strategies on behalf of Microsoft, just as he executed IBM's global strategies."); *see also Estee Lauder Cos. v. Batra*, 430 F. Supp. 2d 158, 174 (S.D.N.Y. 2006) (Even though "a trade secret has not yet been disclosed, irreparable harm may be found based upon a finding that trade secrets will inevitably be disclosed where, as here, the movant competes directly with the prospective employer and the transient employee possesses highly confidential or technical knowledge[.]").

According to Kim's LinkedIn profile, Kim is a Senior Software Engineer, Flight Control at Skyryse since December 2021 and "Skyryse is developing FlightOS, the world's first universal flight deck and operating system," (*see* www.linkedin.com/in/misook-kim-8292837)--*precisely* the same role and responsibilities that Kim was performing for Moog. (Hunter Dec. ¶¶ 31, 34). This conclusion is bolstered by the fact that Kim (at Pilkington's instructions and with Skyryse's knowledge) actually copied "100% of the base Platform software and code (i.e., "[a]ll three iterations (commercial, military, motors) of Platform were copied, as well as test artifacts related to the iterations," (Hunter Dec., ¶ 45), which "demonstrates defendants' cavalier attitude toward their duties to their former employer" and "gives rise to a reasonable inference that they would use [Moog's] confidential information against it." *See Integrated Cash Mgmt. Servs., Inc v. Digital Transactions, Inc*., 920 F.2d 171, 172 (2nd Cir. 1990) (permanently enjoining

defendants from using plaintiff's trade secrets because of the "cavalier way in which the defendants treated their secrecy and nondisclosure obligations," despite the fact that there was "no proof that the copied files were directly used").

Third, Moog's confidential information and trade secrets would unquestionably be valuable to Skyryse because they would save Skyryse "tens of millions of dollars and several years of developing that software" in avoided development costs. (Hunter Dec., ¶ 59); *cf. Lima*, 2020 WL 5261336, at *13 ("The record […] reflects that knowledge of the trade secrets at issue would be valuable to Microsoft."). Fourth, "the nature of the industry" is highly-competitive and one in which millions of dollars and years of work are spent developing and testing confidential and proprietary software. Companies like Moog that have an established, tested, and proven software and that have successfully delivered on contracts have a "huge competitive advantage" because "other competitors do not have [Moog's] level of adaptable base software which allows project-specific applications to be developed so quickly on top of any existing base software," which in turn allows Moog to be the "front runner" in bidding on and winning contracts with government and commercial parties. (Hunter Dec., ¶ 13); *cf. Lima*, 2020 WL 5261336, at *13 (The nature of the industry is "very competitive" because competitors "engage the same clients[.]").

In short, even if the Court finds there was no proof of actual misappropriation now at the inception of the case, Moog is entitled to a preliminary injunction against Defendants based on the inevitable disclosure doctrine.[3]

[3] This conclusion is supported by Section 8 of the 2018 and 2019 NDAs between Skyryse and Moog, which provide that a breach thereunder will result in "irreparable and continuing damage" and that the "non-breaching Party shall be entitled to seek injunctive relief." (Stoelting Dec., Exs. A, B). "Where, as here, the agreed-to language of a restrictive covenant explicitly provides that a breach by the employee will constitute irreparable harm to the employer, [courts in the Second Circuit] have found that fact sufficient to discharge the movant's burden of showing irreparable harm for purposes of a preliminary injunction." *Devos, Ltd. v. Record*, No. 15-CV-6916(ADS)(AYS), 2015 WL 9593616, at *8 (E.D.N.Y. Dec. 24, 2015).

III. MOOG IS HIGHLY LIKELY TO SUCCEED ON ITS CLAIMS

A Violation of the Defend Trade Secrets Act

To prevail on a DTSA claim, a plaintiff must show "an unconsented disclosure or use of a trade secret by one who (i) used improper means to acquire the secret, or (ii) at the time of disclosure, knew or had reason to know that the trade secret was acquired through improper means, under circumstances giving rise to a duty to maintain the secrecy of the trade secret, or derived from or through a person who owed such a duty." *Elsevier Inc. v. Doctor Evidence, LLC*, No. 17-cv-5540 (KBF), 2018 WL 557906, at *3 (S.D.N.Y. Jan. 23, 2018). Under the DTSA, a trade secret is information that "derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person . . ." 18 U.S.C. § 1839(3)(B). To qualify as trade secret, the owner must have "taken reasonable measures to keep such information secret." 18 U.S.C. § 1839(3)(A). Moog can satisfy these elements and is likely to succeed on its DTSA claim.

First, the trade secret information at issue is Moog's source code for Platform software and related project-specific applications and programs, and the SEPG checklists and documents to ensure the software will meet certification requirements of aviation authorities around the world. As demonstrated above, this information has enormous economic value and provides Moog a large competitive advantage in the marketplace. (Hunter Dec., ¶ 13).

Second, Moog takes reasonable steps to keep its information secret, including (i) maintaining controlled access to its buildings and security screening and background checks for employees prior to hiring; (ii) requiring employees to acknowledge and comply with employee handbooks which prohibit disclosure or copying of Moog's confidential information; (iii) robust written policies regarding Moog's proprietary and trade secret information; (iv) requiring software engineers to complete extensive trainings regarding company "trade secrets"; (v)

housing Platform, including all attendant project-specific software, on a secure server; (vi) limiting access to the software database to a "need to know" basis requiring five levels of credentials; (vii) requiring departing Moog employees to sign an exit form affirming no access or copies of such materials and that they will not breach their fiduciary duties to Moog; (viii) designating all Moog source code files as proprietary and confidential; and (ix) entering into NDAs with third parties to protect Moog confidential information. (Hunter Dec., ¶¶ 19-29).

Third, Moog has established Defendants' misappropriation under 18 U.S.C. section 1839(5). Kim copied "100% of the base Platform software and code" *less than one week* after Pilkington went to work for Skyryse and *less than one month* before Kim went to work with Pilkington at Skyryse. (Hunter Dec., ¶¶ 34, 41). She took the data from Pilkington's branch, which only makes sense if he were directing her. As a senior engineer, Kim clearly *knew* when she copied 100% of Moog's Platform software that she had a duty to maintain its secrecy, which she acknowledged in the Exit Form she signed less than a month after copying all of Moog's data. Kim's confirmed theft of Moog's trade secret information and disclosure to Pilkington and Skyryse is a clear violation of the DTSA. Pilkington and Skyryse have also misappropriated Moog's trade secrets within the meaning of the DTSA because they knew Kim owed Moog a duty to maintain its secrecy (as did Pilkington). *Fabkom, Inc. v. R.W. Smith & Assocs, Inc*., No. 95-cv-4552 (MBM), 1996 WL 531873, at *9 (S.D.N.Y. Sep. 19, 1006) (granting preliminary injunction based on "a web of perhaps ambiguous circumstantial evidence from which the trier of fact may draw inferences which convince him that it is more probable than not that what plaintiffs allege happened did in fact take place," and noting "misuse can rarely be proved by convincing and direct evidence." (internal citations and quotation marks omitted); *Mickey's Linen v. Fischer*, No. 17 C 2154, 2017 WL 3970593, at *12-13 (N.D. Ill. Sept. 8, 2017) (granting injunction upon finding "substantial circumstantial evidence" that the defendant improperly

acquired plaintiff's trade secrets, and a "high probability" that further misappropriation would otherwise ensue).

The forensic analysis of Kim's devices confirms that vast volumes of Moog's data were intentionally deleted to conceal what was copied or where that data was copied or transferred to. (*See generally* Pixley Dec.). Kim also copied additional Moog data on December 15, 2021, deleted voluminous Moog data on her last day at work, and used an unknown and unreturned third hard drive. (*Id*. at ¶¶ 20, 24-27). A false hard drive was even re-named to resemble the actual hard drive used to copy Moog's data. (*Id*. at ¶¶ 31-32). And again, Kim copied "100% of the base Platform software and code" less than a month before quitting Moog to join Pilkington at Skyryse, and with no legitimate reason to do so. (Hunter Dec., ¶¶ 41, 45). This overwhelming evidence of wrongdoing shows Moog is likely to succeed on its DTSA claim.

B Misappropriation of Trade Secrets

"To succeed on a claim for the misappropriation of trade secrets under New York law, a party must demonstrate: (1) that it possessed a trade secret, and (2) that the defendants used that trade secret in breach of an agreement, confidential relationship or duty, or as a result of discovery by improper means." *PLC Trenching*, 2011 WL 13135653, at *4. A trade secret is "any formula, pattern, device or compilation of information which is used in one's business, and which gives the owner an opportunity to obtain an advantage over competitors who do not know or use it." *Freedom Calls Found. v. Bukstel*, 2006 WL 845509, at *15 (E.D.N.Y. Mar. 3, 2006). As explained above, Moog's information at issue is likewise a trade secret under New York law. Moog's source code for Platform software and related project-specific applications, programs, and spreadsheets are information of the kind that is protected under New York law. *See Fabkom*, 1996 WL 531873, at *6-7 (granting an injunction and recognizing that "source code, and the architecture of a computer program" qualify as trade secrets because they are "certainly not

known outside the business" and are "not public knowledge"); *see also Bright Start Furniture, Inc. v. E & B Glob., Inc.*, No. 09-CV-3008 RRM/JMA, 2009 WL 2382304, at *1 (E.D.N.Y. Jul. 31, 2009) (same). As with its DTSA claim, Moog is likely to succeed in showing Defendants misappropriated Moog's trade secrets under New York state law.

C Breach of Contract

To succeed on a breach of contract claim, "a plaintiff must establish: (1) the existence of the contract; (2) the plaintiff's performance under the contract; (3) the defendant's breach of that contract; and (4) resulting damages." *Golden Krust Patties, Inc. v. Bullock*, 957 F. Supp. 2d 186, 197 (E.D.N.Y. 2013) (granting preliminary injunction on claim for breach of employee contract). Here, Moog is likely to succeed on its breach of contract claim. First, there is no dispute Kim signed an Exit Form on her last day at Moog in which she affirmed in writing that she had been "provided access to proprietary information, including, but not limited to, intellectual property, plans, strategies and other trade secret[s]" and affirmed that she did "not maintain access to, or have possession of, any tangible or digital record of Moog IP-whether in hard copy or digital form—on any device, cloud, or digital storage facilities." (Daly Dec. ¶ 4, Ex. A). Similarly, Pilkington and Kim both agreed to comply with Moog's Employee Handbook, which prohibits the disclosure or copying of Moog's proprietary information. (Hunter Dec. ¶ 21, Exs. A, B).

Second, Moog has not done anything contrary to the Employee Handbook or Exit Form. Third, Kim copied 100% of Moog's Platform software and other proprietary information at Pilkington and Skyryse's instruction less than a month before joining Skyryse in breach of the Exit Form and Employee Handbook, and Moog has unquestionably been damaged as a result.[4]

[4] Moog's breach of contract claims against Pilkington and Kim are not dependent on their contractual confidentiality obligations. "As employees of [Moog,] defendants [Pilkington and Kim] owed their employer a duty not to divulge confidential information, therefore it is not necessary to determine the viability of the confidentiality agreements[.]" *DoubleClick Inc. v. Henderson*, No. 116914/97, 1997 WL 731413, at *4 (N.Y. Sup. Ct. Nov. 7, 1997).

Moog is likely to prevail on its breach of contract claim. *See Computer Assocs. Int'l Inc. v. Bryan*, 784 F. Supp. 982, 1009-1010 (E.D.N.Y. 1992) (granting a preliminary injunction against a former employee because he "essentially copied" his former employer's software in violation of his confidentiality agreement and fiduciary duties owed to his former employer).

D Breach of Fiduciary Duty and Aiding and Abetting

The elements of a claim for breach of fiduciary duty under New York law are "(1) the existence of a fiduciary relationship, (2) misconduct by the defendant, and (3) damages directly caused by the defendant's misconduct." *PLC Trenching Co., LLC*, 2011 WL 13135653, at *8. Under New York law, an at-will employee owes his or her employer a fiduciary duty of loyalty, including a duty not to disclose or use the employer's proprietary or confidential information to compete with their employer. *Id*. A claim for aiding and abetting a breach of fiduciary duty requires "(1) a breach of a fiduciary of obligations to another, (2) that the defendant knowingly induced or participated in a breach, and (3) that plaintiff suffered damages as a result of the breach." *Obeid v. Mack*, No. 14CV6498-LTS-MHD, 2016 WL 5719779, at *5 (S.D.N.Y. Sep. 30, 2016). The defendant must also have actual knowledge of the breach and have substantially assisted the primary violator. *Id*.

Here, Pilkington and Kim each owed Moog a fiduciary duty of loyalty not to misuse or disclose Moog's confidential and proprietary information or use Moog's information in order to compete with Moog. In breach of their duties, however, Pilkington (and thus Skyryse) instructed Kim to misappropriate, and Kim in fact did misappropriate, "100% of [Moog's] base Platform software" less than one week after Pilkington went to work for Skyryse and less than one month after Kim followed Pilkington to Skyryse. (Hunter Dec., ¶¶ 41, 45). Kim's use of Pilkington's file path to copy Moog's data shows that Pilkington aided and abetted Kim's breach of fiduciary duty with actual knowledge. (*Id*., ¶ 47). Moog is likely to prevail on its breach

of fiduciary duty claims against Pilkington and Kim. *Bryan*, 784 F. Supp. at 1009-1010.[5]

IV. BALANCE OF HARDSHIPS WEIGHS DECIDEDLY IN FAVOR OF MOOG

Moog has demonstrated a high likelihood of success on the merits of its claims, so there is no need for the Court to balance the hardships between the parties. If, however, the Court finds that Moog has only raised a substantial question going to the merits of its claims, the Court should find that the balance of hardships tips decidedly in favor of Moog. Here, Moog is seeking only to preserve the status quo by preventing Defendants from using Moog's trade secrets and other proprietary information that they should never have misappropriated in the first place, which imposes virtually no hardship on Defendants. If, in fact, Defendants did not engage in this theft of data, the restraint on its use causes them no hardship at all. By contrast, if Moog's requested temporary and injunctive relief does not issue, Defendants can continue to exploit and disseminate Moog's trade secrets and proprietary information to compete unfairly with Moog, which creates unbearable hardship on Moog. Consequently, the balance of hardships weighs decidedly in favor of Moog. *See, e.g.*, *Kelly v. Evolution Markets, Inc.*, 626 F. Supp. 2d 364, 376 (S.D.N.Y. 2009*)* (finding that balance of hardships tipped decided in plaintiff's favor where plaintiff faced loss of business); *Natsource LLC*, 151 F.Supp.2d at 472 (finding balance of hardships weighed in favor of plaintiff where plaintiff stood to lose customers, but defendant's ability to earn a livelihood would not be impaired by enforcement of the reasonable restrictive covenant that the parties had agreed to).

CONCLUSION

For the foregoing reasons, Moog requests this Court grant the requested TRO and PI.

[5] Moog is also likely to prevail on its claim for tortious interference with economic advantage. Defendants' copying of nearly all of the files (including coding, testing, and certification files) related to eRTOS and Sensitive Government Program 1, obligates Moog to disclose Kim's data theft, which jeopardizes Moog's prospects for future contracts. Moog has never had to report before. (Hunter Dec., ¶¶ 66-67). This meets every element of the claim. *See JTH Tax, Inc. v. Gouneh*, 721 F. Supp. 2d 132, 139 (N.D.N.Y. 2010) (setting forth the elements of the claim).

Dated: March 7, 2022

SHEPPARD, MULLIN, RICHTER & HAMPTON LLP
Attorneys for Plaintiff Moog Inc.

By: s/Rena Andoh
Rena Andoh
Travis J. Anderson (*pro hac vice* forthcoming)
Tyler E. Baker (*pro hac vice* forthcoming)
Kazim A. Naqvi (*pro hac vice* forthcoming)
30 Rockefeller Plaza
New York, New York 10112
Telephone: (212) 653-8700'

and

HODGSON RUSS LLP

By: s/Robert Fluskey
Robert J. Fluskey, Jr.
Melissa N. Subjeck
Pauline T. Muto
The Guaranty Building
140 Pearl Street, Suite 100
Buffalo, New York 14202
(716) 856-4000